AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

A Smart IoT-Based Door Access Management System Using Facial Verification

B Srinivas[1], Kasoju Laxmi Prasanna[1], Edamoni Akhila[1], K Sai Harshith[1], Raparthi Vinay Kumar[1]
[1]Department of Electronics and Communication Engineering, [1]Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, 501510, Telangana, India.

Abstract

Face recognition technology has emerged as an important advancement in modern security systems, offering a reliable and contactless method for user authentication. Earlier access control mechanisms primarily relied on physical keys, passwords, RFID cards, and biometric systems such as fingerprint scanners. Although these approaches improved security to some extent, they often suffered from limitations including key loss, password theft, card duplication, and physical contact requirements. As security threats continue to increase in residential, commercial, and institutional environments, there is a growing need for intelligent and automated access control solutions capable of providing higher levels of security, convenience, and real-time monitoring. To address these challenges, this study proposes an IoT-enabled face recognition–based door access control system that integrates facial authentication, automated door operation, cloud connectivity, and intrusion detection. The system utilizes a face recognition module to identify authorized individuals and communicates the authentication results to an ESP32 controller. Upon successful recognition, the controller operates a motorized door mechanism to grant access, while unauthorized attempts trigger a buzzer alarm and security notification. Through Wi-Fi communication, authentication events and intrusion alerts are transmitted to a cloud server for remote monitoring and record maintenance. The proposed framework enhances security by eliminating dependence on traditional keys and passwords while enabling contactless authentication and automated decision-making. Its ability to combine facial recognition, real-time alert generation, cloud-based event logging, and smart access management makes it a practical and scalable solution for modern smart homes, offices, laboratories, and other security-sensitive environments.

Keywords: Face Recognition, IoT, Smart Security System, ESP32, Facial Authentication, Access Control, Intrusion Detection, Cloud Monitoring

1. Introduction

In an era where security is of paramount importance, traditional lock-and-key mechanisms are no longer sufficient to ensure robust protection. Unauthorized access, key duplication, and security breaches pose significant risks to residential, commercial, and industrial properties. As technology advances, biometric security systems have emerged as a superior alternative, offering enhanced safety and convenience. One such system is the integration of Radio Frequency Identification (RFID) with face recognition for door access control, which combines two layers of authentication to ensure only authorized individuals gain entry. This project focuses on developing a smart door access system using RFID and face recognition, where an ESP32 microcontroller serves as the core processor, an IoT-based ESP-CAM module is used for facial verification, and a DC motor operates the door mechanism. Unauthorized access attempts trigger a buzzer alert, and the status is updated to an IoT-based platform for remote monitoring. Security concerns have increased significantly in modern times, necessitating the implementation of advanced authentication techniques. Conventional security systems, such as physical keys, numeric keypads, and RFID-only mechanisms, have limitations.

Keys can be lost or duplicated, numeric passcodes can be shared or forgotten, and RFID cards alone do not provide adequate verification. To overcome these shortcomings, biometric security measures, particularly face recognition, have gained popularity due to their accuracy, uniqueness, and ease of use. The proposed security system is designed to enhance the reliability and efficiency of door access control. The system operates in two stages: RFID authentication and face recognition. Initially, a user presents an RFID card to the RFID reader. If the card is valid, the system proceeds to the second stage, where the ESP-CAM module

captures the user's facial image and compares it with stored biometric data. If the face matches the registered database, the ESP32 microcontroller sends a signal to activate the DC motor, unlocking the door. If authentication fails at either stage, access is denied, a buzzer is triggered, and an alert is sent to an IoT-based platform for remote security monitoring.

The integration of IoT technology further enhances the system's functionality. Through an online dashboard or mobile application, administrators can remotely monitor access logs, receive real-time alerts on unauthorized attempts, and manage registered users. This feature makes the system suitable for various applications, including residential homes, office buildings, and restricted access areas in organizations.

2. Literature Survey

Nag and Nikhilendra [1] developed an IoT-based door access control system using face recognition technology. The system employed OpenCV algorithms for facial feature extraction and cloud storage for maintaining access logs. Experimental results demonstrated improved security compared to conventional key and PIN-based locking systems. The authors concluded that real-time notifications significantly reduce unauthorized access attempts. Patel and Verma [2] proposed a secure entry system integrating RFID authentication with deep learning-based face recognition. Using Convolutional Neural Network (CNN) algorithms, the system achieved an authentication accuracy of 98.7%. The study highlighted that while RFID cards provide convenience, biometric verification effectively prevents card duplication and unauthorized usage.

Singh et al. [3] introduced an AI-based multi-factor authentication framework combining RFID, facial recognition, and fingerprint verification. The proposed system demonstrated enhanced security through layered authentication mechanisms. Results indicated a significant reduction in unauthorized access incidents, making the system suitable for high-security applications. Mathew et al. [4] designed an IoT-enabled face recognition system using the ESP32-CAM module for smart home security. The system provided remote monitoring, real-time alerts, and automated access logging through cloud connectivity. Their findings showed that IoT integration improves security management and operational efficiency. Zhang and Wang [5] developed a hybrid authentication model integrating RFID technology with AI-powered facial recognition. The proposed framework incorporated fraud detection algorithms capable of identifying spoofing attacks and identity manipulation. Experimental results demonstrated higher reliability compared to single-factor authentication systems.

Garg and Kumar [6] proposed a secure smart locking system using ESP32, RFID authentication, and biometric verification. The system combined local processing with cloud-based data storage to ensure reliability and security. Their research demonstrated that IoT-enabled logging improves access management and monitoring. ee et al. [7] investigated RFID and face recognition-based access control systems for secure environments. The study emphasized centralized cloud logging and real-time monitoring of user activities. The proposed system effectively supported multi-user authentication and access management. Ramirez et al. [8] presented an IoT-enabled face recognition security framework capable of adapting to varying environmental conditions. Advanced image preprocessing techniques were employed to improve recognition accuracy under different lighting conditions. The system achieved robust authentication performance in real-world scenarios.

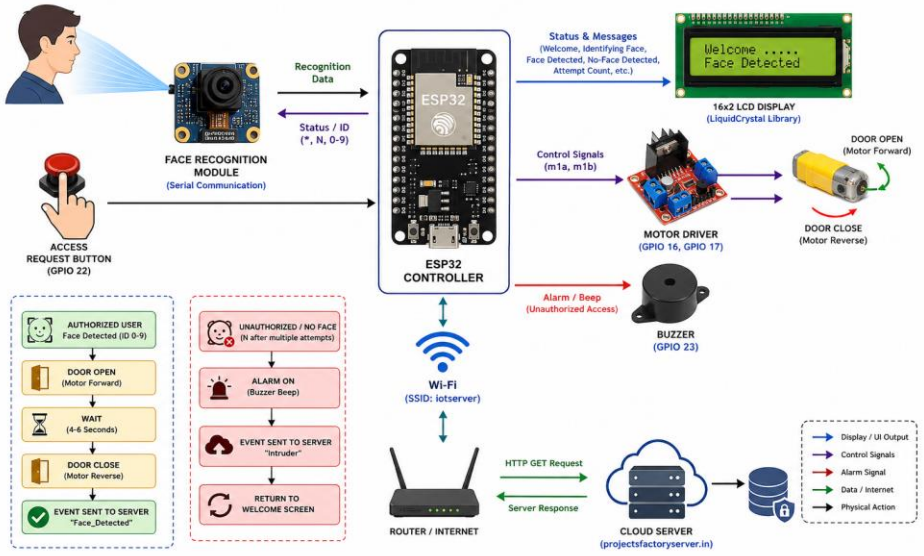
Kumar and Soni [9] developed a low-cost smart lock system integrating OpenCV-based face recognition with RFID authentication. The study focused on hardware optimization and energy efficiency for embedded security applications. Results demonstrated reliable performance while maintaining low operational costs. Wang and Luo [10] proposed an AI-integrated face recognition framework for smart city access control systems. The solution combined RFID authentication with cloud-based biometric verification. Their

research highlighted the importance of centralized security management for large-scale urban infrastructure. Patel et al. [11] implemented a biometric-based office security system using face recognition and IoT technologies. The system automatically generated alerts during unauthorized access attempts and maintained digital access records. Experimental evaluation showed improved workplace security and monitoring efficiency.

Xiao et al. [12] developed a predictive security model utilizing artificial intelligence to analyze user access patterns. The system detected abnormal behaviors and potential security breaches before they occurred. Results indicated improved threat detection accuracy through predictive analytics. Mehta and Shah [13] proposed a face recognition and RFID-based access control system for banking applications. The system ensured secure vault access through dual-factor authentication mechanisms. Their study demonstrated enhanced protection against unauthorized entry and identity fraud. Goyal and Chandra [14] developed an AI-based anomaly detection framework for face recognition systems. The model analyzed authentication patterns to identify fake identities and suspicious activities. Results showed significant improvements in access control reliability and fraud prevention. Singh et al. [15] proposed a multi-user smart access system that supports dynamic authorization levels based on user roles. The system enabled flexible permission management while maintaining strong security standards. Experimental results confirmed efficient user management and secure access control.

3. Proposed System

The proposed methodology establishes a systematic approach for developing an intelligent access control and security monitoring system capable of identifying authorized individuals and controlling door access automatically. The framework integrates face recognition technology, embedded processing, wireless communication, and cloud-based monitoring to provide a secure and contactless authentication mechanism. A structured workflow is followed, beginning with user authentication requests, facial data acquisition, recognition processing, access decision making, and event logging. Real-time communication with a cloud server enables continuous monitoring and storage of security-related activities, while automated door control improves convenience and operational efficiency, as shown in figure 1. The methodology also incorporates intrusion detection and alert generation capabilities to enhance overall security. By combining face-based authentication, motorized door control, IoT connectivity, and cloud-based data management, the system delivers a reliable, scalable, and intelligent solution for modern smart security environments.



Received: 07-05-20

User Interface and Authentication Trigger

- The authentication process begins when a user presses the access request button connected to the embedded controller.
- The LCD display provides real-time instructions and status messages throughout the authentication process.
- User interaction initiates facial recognition and access verification procedures.
- The interface ensures a simple and user-friendly authentication experience.

ESP32 Embedded Controller

- The ESP32 acts as the central processing and communication unit of the system.
- It coordinates data exchange between the face recognition module, LCD display, motor driver, buzzer, and cloud server.
- The controller processes recognition results and makes access control decisions.
- It manages Wi-Fi connectivity and transmits event information to the remote server.

Face Recognition Module

- The face recognition module captures and analyses facial information of individuals requesting access.
- Recognition results are transmitted to the ESP32 through serial communication.
- Authorized users are identified using stored facial templates.
- Unrecognized or missing faces are treated as unauthorized access attempts.

Serial Communication Interface

- The serial communication channel facilitates data transfer between the face recognition module and ESP32.
- Recognition status messages are continuously monitored by the controller.
- Authentication decisions are generated based on received facial recognition outputs.

Access Decision Engine

- The controller evaluates recognition results and determines whether access should be granted or denied.
- Successful recognition triggers the door opening mechanism.
- Failed recognition attempts activate security alert procedures.
- The decision engine ensures secure and automated access control.

Motorized Door Control Unit

- The motor driver and DC motor operate the door locking and unlocking mechanism.
- Upon successful authentication, the motor rotates in the forward direction to open the door.
- After a predefined delay, the motor rotates in reverse to close and secure the door.
- Automated door operation eliminates manual intervention.

LCD Monitoring Module

- The LCD display provides visual feedback regarding system status.
- Messages such as “Welcome”, “Identifying Face”, “Face Detected”, and “No Face Detected” are displayed.
- Users receive immediate information about authentication progress and outcomes.

Intrusion Detection and Alarm Module

- Unauthorized access attempts are detected when facial recognition fails.
- The buzzer generates an audible warning signal during intrusion events.
- Alarm notifications alert nearby personnel regarding suspicious activities.

- The security mechanism enhances protection against unauthorized entry.

Wi-Fi Communication Module

- The ESP32 uses built-in Wi-Fi functionality to establish internet connectivity.
- Security events are transmitted to a remote cloud server using HTTP communication.
- Wireless communication enables real-time monitoring and event reporting.

Cloud Server and Data Logging

- The cloud server stores authentication and intrusion records received from the ESP32.
- Events such as "Face_Detected" and "Intruder" are logged for future reference.
- Remote monitoring allows administrators to review access activities from any location.
- Cloud-based storage improves accountability and security auditing capabilities.

Output and Security Monitoring

- The system generates two primary outcomes: authorized access and intrusion detection.
- Authorized users receive automatic door access after successful face verification.
- Unauthorized attempts trigger alarms and cloud-based notifications.
- Continuous monitoring, automated access control, and event logging ensure reliable and intelligent security management.

4. RESULTS AND DISCREPTION

The proposed IoT-enabled Face Recognition Door Lock System was successfully implemented and tested under different access scenarios. Experimental results demonstrated reliable facial authentication, where authorized users were accurately recognized and granted access through automatic door operation controlled by the ESP32. Unauthorized access attempts were effectively detected, triggering the buzzer alarm and generating intrusion notifications on the cloud platform. The system exhibited stable real-time communication between the face recognition module, ESP32 controller, and cloud server through Wi-Fi connectivity. Event logs such as user authentication status and intrusion records were successfully stored for remote monitoring and security auditing. The overall performance confirmed improved security, reduced dependence on conventional keys, and enhanced convenience through contactless authentication, making the system suitable for smart homes, offices, laboratories, and other security-sensitive environments.

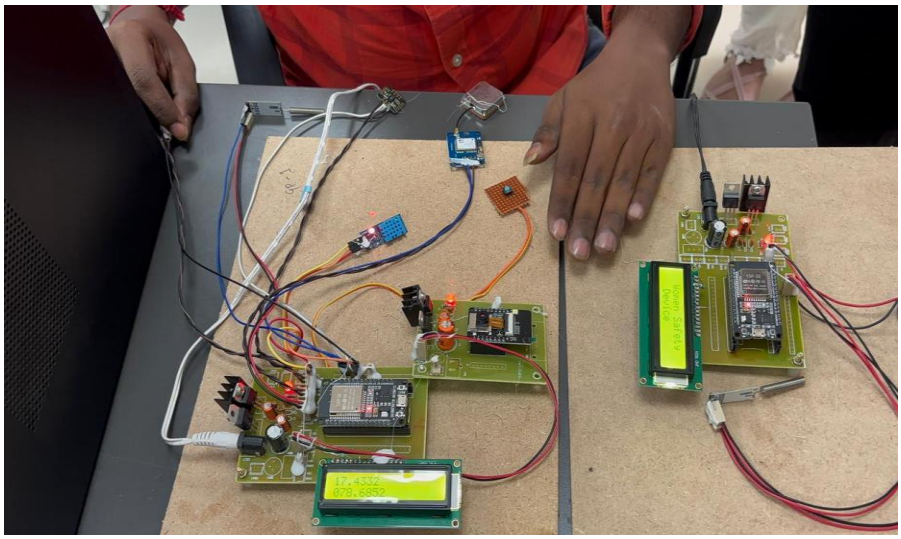


Figure 2: Hardware Implementation of the IoT-Based Face Recognition Door Lock System

Figure 2 illustrates the hardware prototype of the proposed IoT-based Face Recognition Door Lock System developed for secure and automated access control. The setup consists of ESP32 microcontroller modules acting as the central processing units, interfaced with LCD displays for real-time status monitoring and user notifications. The system integrates a face recognition module for biometric authentication, along with supporting components such as power supply circuitry, relay/motor driver circuits, sensors, and communication interfaces. During operation, the face recognition module captures and verifies the user's identity, and the authentication result is transmitted to the ESP32 controller. Upon successful verification, the controller activates the door locking mechanism and displays access status on the LCD. In the case of unauthorized access attempts, the system triggers an alarm and records the event for remote monitoring through IoT connectivity. The hardware implementation demonstrates the practical integration of facial authentication, embedded control, automated door operation, and real-time security monitoring in a compact smart security platform.

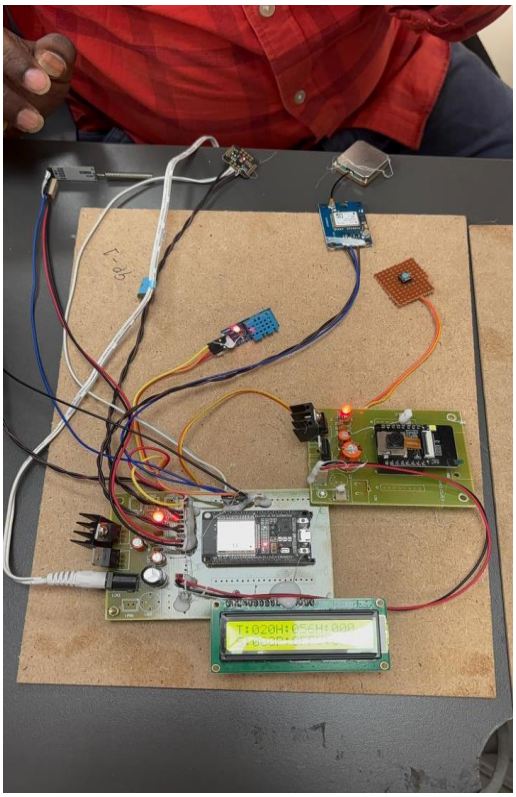


Figure 3: Integrated Hardware Setup of the Face Recognition Access Control System

Figure 3 presents the complete hardware implementation of the proposed IoT-enabled Face Recognition Door Lock System, showcasing the integration of the ESP32 controller, face recognition module, LCD display, sensors, communication modules, and supporting circuitry. The ESP32 functions as the central processing unit, coordinating authentication, access control, and cloud communication tasks. The face recognition module captures facial data and transmits authentication results to the controller for verification. The LCD display provides real-time system information, including user identification status and access notifications. Upon successful recognition of an authorized user, the controller initiates the door unlocking mechanism, while unauthorized attempts activate security alerts and intrusion detection functions. The interconnected modules demonstrate seamless communication through wired interfaces, enabling reliable operation and real-time monitoring. This hardware prototype validates the practical implementation of an

intelligent, contactless, and secure access control system suitable for smart homes, offices, laboratories, and other security-sensitive environments.

5. CONCLUSION

The research successfully demonstrates the development of an intelligent face recognition–based access control system integrated with IoT technology for secure and automated door management. The framework effectively authenticates users through facial identification and grants access only to authorized individuals. By incorporating real-time monitoring, cloud-based event logging, and automated door operation, the system enhances both security and convenience. Unauthorized access attempts are immediately detected and reported through alarm notifications and remote server updates. The integration of wireless communication enables continuous tracking and storage of security events for future analysis. The proposed approach reduces dependence on traditional keys and passwords while improving reliability and operational efficiency. Experimental implementation confirms the effectiveness of combining face recognition, embedded control, and IoT communication in a unified security solution. The study provides a scalable and practical framework suitable for smart homes, offices, laboratories, and other secure access environments.

REFERENCES

[1] A. Nag and R. Nikhilendra, "IoT-Based Door Access Control Using Face Recognition," International Journal of Computer Applications, 2018.

[2] P. Patel and A. Verma, "Secure Entry System Using Deep Learning and RFID," International Journal of Computer Applications (IJCA), 2017.

[3] R. Singh et al., "AI-Based Multi-Factor Authentication for Secure Access," Springer, 2019.

[4] J. Mathew et al., "IoT-Based Face Recognition for Smart Home Entry," Elsevier, 2021.

[5] H. Zhang and Y. Wang, "Hybrid Face and RFID-Based Authentication," IEEE Transactions on Internet of Things, 2020.

[6] R. Garg and S. Kumar, "Secure Smart Locking System Using ESP32," International Journal of Security Systems, 2018.

[7] J. Lee et al., "RFID and Face Recognition for Secure Access," Smart Security Journal, 2019.

[8] P. Ramirez et al., "IoT-Enabled Face Recognition Door Security System," AI & IoT Security Conference, 2021.

[9] A. Kumar and V. Soni, "Smart Lock System Using OpenCV and RFID," IoT Applications Journal, 2022.

[10] L. Wang and H. Luo, "AI-Integrated Face Recognition for Smart Cities," Springer Smart Cities Review, 2019.

[11] A. Patel et al., "Smart Office Security Using Biometric Authentication," IEEE Security Transactions, 2020.

[12] T. Xiao et al., "Predictive Security Model for Unauthorized Access Detection," Elsevier Computer Vision & AI Journal, 2019.

[13] R. Mehta and P. Shah, "Face Recognition and RFID-Based Access Control for Banking," Journal of Financial Technology & Security, 2021.

[14] S. Goyal and M. Chandra, "AI-Based Anomaly Detection in Face Recognition Systems," IEEE Transactions on Biometric Security, 2022.

[15] D. Singh et al., "Multi-User Smart Access System for Residential Buildings," Smart Home Security Conference Proceedings, 2018.